AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently amended) A ~~graphical user interface rendered on~~ computer system ~~a display device~~ configured to display a graphical ~~the graphical~~ user interface for configuring a new service ~~detection process~~alert rule, the graphical user interface comprising:

a first field that ~~depicts choices for entities~~allows a user to specify an entity to track in the network;

a second field that allows the user to specify ~~a system to track if the selected entity is providing or consuming a service~~whether the rule is to be applied when the specified entity is providing or consuming a new service;

a third field that ~~depicts a range over which to track an entity selected in the first field~~allows the user to specify a range of network entities to which the new service is unprecedented; and

a fourth field that allows the user to specify a severity for an alert generated if a new service is detected.

2. (Currently amended) The ~~graphical user interface~~computer system of claim 1 wherein the fields are linguistically tied together on the interface to form a sentence that corresponds to a rule.

3. (Currently amended) The ~~graphical user interface~~computer system of claim 1 further comprising:

a list of new service detection rules stored in the detection system.

4. (Currently amended) The ~~graphical user interface~~computer system of claim 1 wherein the first field allows a user to specify the entity to track as "a specific host", "any host in a specific role", "any host in a specific segment" or "any host."

5. (Currently amended) The ~~graphical user interface~~computer system of claim 1 wherein the third field specifies details for the extent of the comparison for the entity specified in the first field as "host", "in its role", "in its segment" or "anywhere" in the network.

6. (Currently amended) The ~~graphical user interface~~computer system of claim 1 wherein event severity is a numerical value entered by the user.

7. (Currently amended) The ~~graphical user interface~~computer system of claim 1 wherein the fields are implemented as pull-down fields.

8. (Currently amended) A method for detection of a new service involving a host in a network, the method comprises:

retrieving a baseline list of port and/or service protocols used by a host being tracked, the baseline list listing service and/or port protocols used by that host over a baseline period that is of a longer duration ~~that~~ than a current period;

retrieving a current list of service and/or port protocols for the current period used by the host being tracked;

determining whether there is a difference in the protocols, by finding a protocol that was in the current list but was not in the baseline list; and if there is a difference;

determining whether the host is providing or using the new service;

identifying an alert rule corresponding to whether the host is providing or using the new service; and

issuing an alert based at least on the identified alert rule and whether the host is providing or using the new service.~~indicating a new service involving the tracked host.~~

9. (Currently amended) The method of claim 8 further comprising:

determining if the host is ~~providing~~ sending traffic using a protocol not in the current list or ~~using the new service~~receiving traffic with a protocol not in the current list.

10. (Cancelled)

11. (Currently amended) The method of ~~claim 10~~claim 9 further comprising:

retrieving a value corresponding to ~~the alert~~an alert severity level set for violation of the rule.

12. (Previously presented) The method of claim 8 wherein a property of the host being tracked is that the host is at least one of a specific host, any host in a specific role, any host in a specific segment, or any host.

13. (Previously presented) The method of claim 8 wherein the extent of the determining is configured for that host, in its role, in its segment or anywhere in the network.

14. (Original) The method of claim 8 wherein the baseline and current lists of protocols are provided from data in a connection table.

15. (Currently amended) A computer program product residing on a computer readable medium for detection of new services in a network, the computer program product comprising instructions for causing a computer to:

retrieve a baseline list of port and/or service protocols used by a host being tracked, the baseline list listing service and/or port protocols used by that host over a baseline period that is of a longer duration that a current period;

aggregating communication information between every host pair;

retrieve a current list of service and/or port protocols for the current period used by the host being tracked;

determine whether there is a difference in the protocols, by identifying a protocol that was in ~~a~~ the current list but was not in the baseline list; and if there is a difference;

determine whether the host is providing or using the new service;

identify an alert rule corresponding to whether the host is providing or using the new service; and

issue an alert based at least on the identified alert rule and whether the host is providing or using the new service.~~indicate a new service involving the tracked host.~~

16. (Currently amended) The computer program product of claim 15 further comprising instructions to:

determine if the host is ~~providing~~ sending traffic using a protocol not in the current list or ~~using the new service~~receiving traffic with a protocol not in the current list.

17. (Cancelled)

18. (Original) The computer program product of claim 15 wherein instructions to indicate further comprise instructions to:

issue an alert if the new service is detected.

19. (Previously presented) The computer program product of ~~claim17~~ claim 15 further comprising instructions to:

retrieve a value corresponding to the alert severity level set for violation of the rule.

20. (Previously presented) The computer program product of claim 15 wherein a property of the host being track is that the host is at least one of a specific host, any host in a specific role, any host in a specific segment, or any host.

21. (Previously presented) The computer program product of claim 15 wherein the extent of the determining is configured to for that host, in its role, in its segment or anywhere in the network.

22. (Original) The computer program product of claim 15 further comprising instructions to:

access a connection table to provide data for the baseline and current lists of protocols.